CLFE, Certified Lead Forensics Examiner, certification informatique judiciaire, récupération et analyse des preuves

★★★★★

PL-42 **5 Jours (35 Heures)**

Description

Le défi de l'investigation légale informatique est de trouver les données, les collecter et les présenter devant une cour de justice. Ce cours intensif permet aux participants de développer l'expertise nécessaire pour relever ce défi et aussi de passer l'examen de certification officiel, accrédité par PECB.

À qui s'adresse cette formation ?

Pour qui

Spécialiste investigation informatique, analyste de données, spécialiste en recherche et récupération de preuves informatiques, membre d'équipe sécurité, consultant, analyste de media électronique.

Prérequis

Aucun

Les objectifs de la formation

- Comprendre les principes scientifiques spécifiques à l'investigation informatique
- Expliquer la structure des ordinateurs et des systèmes d'exploitation
- Expliquer l'investigation réseau, Cloud et appareils mobiles
- Maîtriser les outils et les méthodologies d'investigation

Programme de la formation

Principes scientifiques spécifiques à l'investigation informatique

- Présentation des principes scientifiques spécifiques à l'investigation informatique.
- Introduction à l'approche de l'investigation informatique.
- Principes fondamentaux.
- Analyse et mise en oeuvre des opérations d'analyse.
- Préparation et exécution des procédures d'investigation.

Structure des ordinateurs et des systèmes d'exploitation

- Identification et sélection des composants d'un ordinateur.
- Identification et sélection des périphériques et autres composants.
- Compréhension des systèmes d'exploitation (OS).
- Extraction et analyse des structures de fichiers.

Investigation réseau, Cloud et appareils mobiles

- Comprendre les réseaux, le Cloud et les environnements virtuels.
- Méthodes génériques pour l'extraction de données dans un environnement virtuel.
- Examen d'un téléphone mobile ou d'une tablette.
- Stockage des informations sur les appareils mobiles.

Outils et méthodologies d'investigation

- Enumération et examen des composants matériels et logiciels des ordinateurs.
- Choix et test des technologies d'investigation.
- Analyse et sélection des procédures adaptées pour les opérations d'investigation.
- Découverte, documentation et retour des preuves sur site.
- Analyse et prise en compte du contexte.

Outils et méthodologies d'investigation

- Enumération et examen des composants matériels et logiciels des ordinateurs.
- Choix et test des technologies d'investigation.
- Analyse et sélection des procédures adaptées pour les opérations d'investigation.
- Découverte, documentation et retour des preuves sur site.
- Analyse et prise en compte du contexte.

Examen de certification

- Domaine 1 : principes scientifiques spécifiques à l'investigation informatique.
- Domaine 2 : principes fondamentaux de l'investigation informatique.
- Domaine 3 : structure des ordinateurs.
- Domaine 4 : systèmes d'exploitation et structures de fichier.
- Domaine 5 : investigation des réseaux, dans le Cloud ou dans les environnements virtuels.
- Domaine 6 : investigation réseau et des appareils mobiles.
- Domaine 7 : outils et méthodologies d'investigation.
- Domaine 8 : examen, acquisition et préservation des preuves électroniques.
- Examen Examen de 3 heures.